UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/882,978	06/15/2001	Jean-Marc Villaret	10013263-1	1005

7590	02/03/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
OYEBISI, OJO O

ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 02/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/882,978	VILLARET ET AL.
	Examiner	Art Unit	
	OJO O. OYEBISI	3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>06/29/04</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-20</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-20</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>15 June 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>07/01/02, 06/29/04</u>.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by
> another filed in the United States before the invention by the applicant for patent or (2) a patent
> granted on an application for patent by another filed in the United States before the invention by the
> applicant for patent, except that an international application filed under the treaty defined in section
> 351(a) shall have the effects for purposes of this subsection of an application filed in the United States
> only if the international application designated the United States and was published under Article 21(2)
> of such treaty in the English language.

2.   Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Davis et

al (Davis hereinafter, US PAT: 6,105,008).

Re claim 1. Davis discloses a method for authenticating an electronic transaction

comprising: inputting smart card information from a smart card into a payment enabled

device (see abstract, also see col.8, lines 11-32); inputting an identification number into

the payment enabled device (i.e., By way of example, security precautions may include

simple **PIN** numbers, biometrics, simple algorithms, or sophisticated algorithms such

as the Data Encryption Standard (DES) or Rivest, Shamir, Adelman (RSA) encryption.

The card is thus able to use these precautions to verify users, card readers, see col. 7

line 65 through col.8 line 5); authenticating the smart card information (i.e., In step 608

the client module of the client terminal interacts with stored-value card 5 to obtain card

information 308 in order to build a draw request message for later transmission 310 to

payment server 206. In one embodiment of the invention, the client applet loads a

local DLL, makes an API call to that library, which in turn makes a call to another DLL

that finally makes a call to the card reader. In this fashion communication with the card

is achieved. Once responses from the card are received, the client module will also

combine these responses into a byte stream suitable for transmission over a network

to a payment server. **Also at this point, the currency type and expiration date on**

the card are checked, and the total cost of the ordered merchandise is checked

against the card balance to ensure that the value on the card is great enough to

cover the transaction. If the checks are not successful, a message to that effect

is delivered to the user and this transaction terminates, see col.12 lines 25-43,

also see col.14, lines 7-20); authenticating the identification number (i.e., A processor

card may include an encryption module in order to provide a variety of security

precautions. By way of example, security precautions may include simple **PIN**

numbers, biometrics, simple algorithms, or sophisticated algorithms such as the Data

Encryption Standard (DES) or Rivest, Shamir, Adelman (RSA) encryption. **The card is**

thus able to use these precautions to verify users, card readers, etc., to validate

security cards and/or to provide a unique signature. Preferably card 5 includes any

number of keys known to the card issuer that are used during the course of a payment

or load transaction to generate signatures for validation of the stored-value card,

validation of the security card or module, and validation of the system itself, see col. 7

line 65 through col.8 lines 10); and sending payment information from a server to a

desired location after authenticating the smart card information and authenticating the

identification number (see abstract)

Re claims 2 and 3. Davis further discloses the method, further comprising: using a

payment enabled devices from the group consisting of a private payment enabled

device and a public payment enabled device (i.e., Client terminal 204 is any suitable

device for interacting with a stored-valued card 5 and for communicating over a

network to a payment server or a merchant server. By way of example, client terminal

204 may be a mainframe computer, a work station, a personal computer, a kiosk, or

any type of service payment terminal that a consumer might use to purchase goods

and/or services. Furthermore, client terminal 204 may also be embodied in any

portable device such as a laptop computer, a cellular telephone, or any variety

of a personal digital assistant (PDA) such as those made by Apple Computer,

Inc. or by U.S. Robotics. Card reader 210 is any suitable interface device

that functions to transfer information and commands between client terminal 204

and stored-value card 5. By way of example, card reader 210 may be a card

reader manufactured by Fischer-Farr International of Naples, Fla., by

Hewlett-Packard of Palo Alto, Calif., by Schlumberger, by Gem Plus, etc. Card

reader 210 may take any variety of forms such as a stand alone unit, integrated

with the client terminal, attached to the keyboard of the client terminal, or

even built in to a floppy disk-sized unit capable of being read from a disk

drive of the client terminal, see col.8 lines 10-32).

Re claim 4. Davis further discloses the method wherein the step of authenticating the

smart card information is performed by the payment-enabled device (i.e., the payment

server receives incoming message and creates a log and updates……., the payment

server then directs this received message to the security card in the terminal as

indicated at 324. Next,..., **the security card processes this response from the**

client's terminal and verifies the stored-value card signature, see col.14 lines 7-

20).

Re claim 5. Davis further discloses the method, wherein the step of authenticating the

smart card information is performed by the server (i.e., merchant server, see col.19

lines 6-30)

Re claim 6. Davis further discloses the method wherein the step of authenticating the

identification number is performed by the smart card (i.e., A processor card may

include an encryption module in order to provide a variety of security precautions. By

way of example, security precautions may include simple **PIN** numbers, biometrics,

simple algorithms, or sophisticated algorithms such as the Data Encryption Standard

(DES) or Rivest, Shamir, Adelman (RSA) encryption. **The card is thus able to use**

these precautions to verify users, card readers, etc., to validate security cards

and/or to provide a unique signature, see col. 7 line 65 through col.8 lines 5)

 Re claim 7. Davis further discloses the method wherein the electronic transaction is

payment for at least one of a good and a service that is being provided by a merchant

(see abstract, also see col.11 lines 43-67)

Re claim 8. Davis further discloses the method wherein the desired location is the

merchant (see abstract)

Re claim 9. Davis further discloses the method wherein the desired location is a

merchant server that is used by the merchant (see abstract)

Re claim 10. Davis further discloses the method wherein the desired location is a

financial institution that is used by the merchant (see col.11 lines 25-40).

Re claim 11. Davis further discloses the method further comprising: sending a

payment request to the server; wherein the payment request includes an amount of

money, a merchant identification number, and smart card owner information (see

col.12 lines 52-67).

Re claim 12. Davis further discloses the method wherein the payment request further

includes an information related to a type of the at least one of a good and a service

(i.e., the transaction identifier see col.12 lines 52-67).

Re claim 13. Davis further discloses wherein the payment request further includes type

of payment information; wherein the type of payment is selected from the group

consisting of: credit, debit, pre-paid, and loyalty point (i.e., the transaction identifier see

col.12 lines 52-67).

Re claim 14. Davis further discloses the method further comprising: issuing a receipt

for the transaction (col.11 lines 25-30).

Re claim 15. Claim 15 recites similar limitations to claim 1 and thus rejected using the

same art and rationale in the rejection of claim 1.

Re claim 16. Claim 16 recites similar limitations to claim 7 and thus rejected using the

same art and rationale in the rejection of claim 7.

Re claim 17. Davis further discloses the system wherein the desired location is one

location selected from the group consisting of: the merchant, a merchant server that is

used by the merchant, and a financial institution that is used by the merchant (see

abstract).

Re claim 18. Claim 18 recites similar limitations to claim 11 and thus rejected using the

same art and rationale in the rejection of claim 11.

Re claim 19. Claim 19 recites similar limitations to claim 12 and thus rejected using the

same art and rationale in the rejection of claim 12.

Re claim 20. Claim 20 recites similar limitations to claim 13 and thus rejected using the

same art and rationale in the rejection of claim 13.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to OJO O. OYEBISI whose telephone number is (571)

272-8298. The examiner can normally be reached on 8:30A.M-5:30P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, HYUNG S. SOUGH can be reached on (571)272-6799. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

***

HYUNG SOUGH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600